U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Effective Practices that Establish Adequate Cyber Security

Beth Reed, Security Specialist
Research and Test Reactor Oversight Branch
Nuclear Regulatory Commission

William T. Shaw
Nuclear Regulatory Commission, Contractor

October 6, 2015

NRC Objective

- In 2013/14 the NRC, in cooperation with TRTR, surveyed licensees to determine the extent of digital technology and potential cyber security risks at NPRs
- The survey determined that cyber security is not currently a risk, but that it could become one in the future
- It was decided that providing recommendations on effective practices to help guide future migration onto digital platforms could ensure that adequate cyber security is maintained

Effective Practices

- To that end the NRC has developed an "Effective Practices" document that offers a wide range of suggestions regarding conversion to and adoption of digital technologies for reactor operation and safety in a manner that preserves cyber security

NRC Document

- Written in plain English
- Lots of illustrations
- Effective practices accompany explanations of their justification
- Possible approaches offered as suggestions
- TRTR engagement

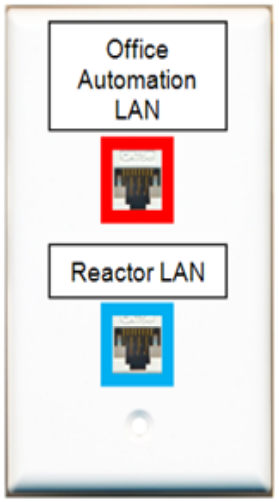
Executive Summary

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

This document provides a consolidation of the effective practices identified among the NPR licensees and also provides guidance for the future to ensure that NPR licensees understand the cyber security issues and consequences (and how to remain cyber-secure) as they migrate onto modern digital platforms and integrate more digital assets into their operations.

Effective Practices

- These effective practices come from observations made at some of the NPR sites surveyed as well as from IT* and Industrial Automation standards and practices for establishing and maintaining adequate cyber security
- The effective practices range from simple suggestions (such as using different colored Ethernet cables and connectors to identify LAN segments that contain sensitive assets) to highly technical ones such as using VLAN technology



*NIST SP 800-53, ISA SP-100 and ISO 27001

Critical Digital Assets

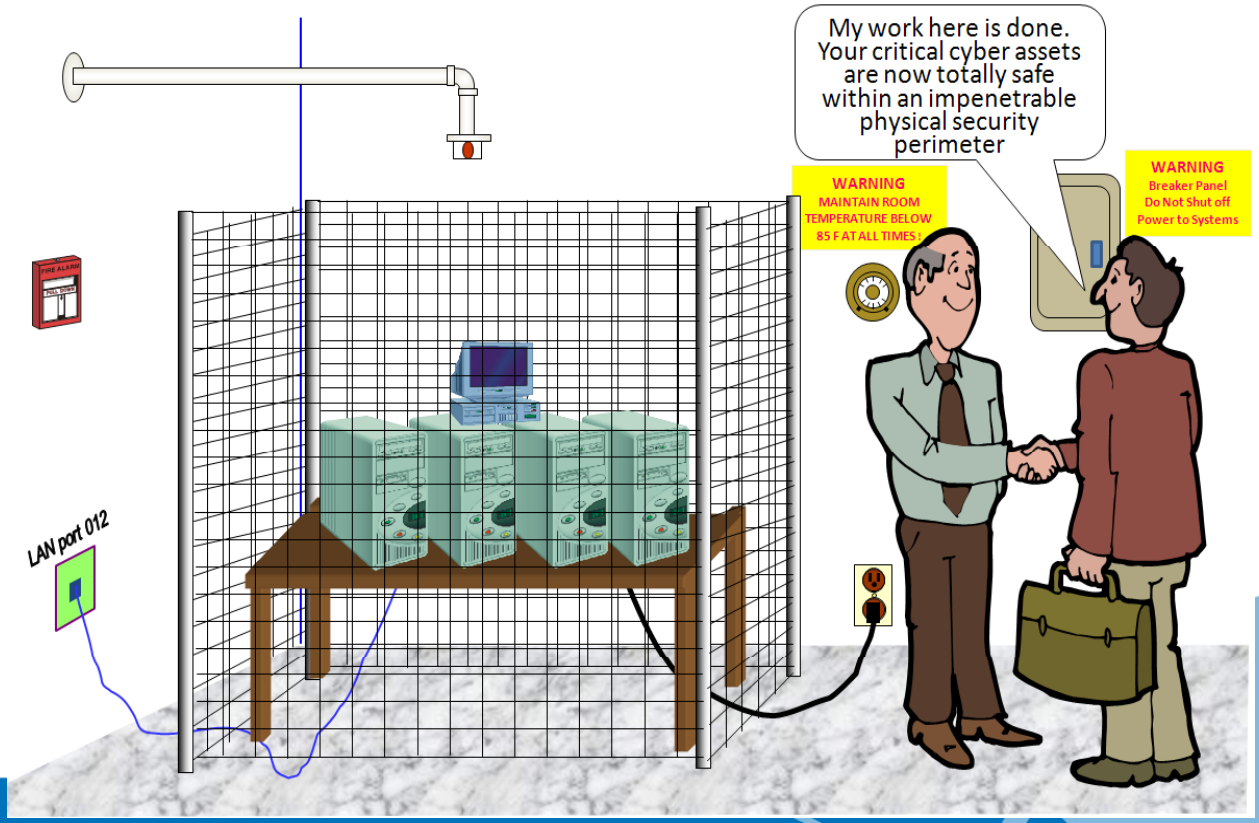
Digital systems and devices that are used to perform or support the functions listed below (a.k.a. - "critical digital assets" or "CDAs") need adequate protection against cyber attacks and malicious manipulation

Functions/Activities of Concern
Physical security of the NPR facility
Detection of unsafe/unauthorized conditions
Personnel access monitoring and control
Reactor safety
Reactor operational control
Emergency response/communications
Storage and protection of SGI
Accurate inventory/location of nuclear materials

Physical Security

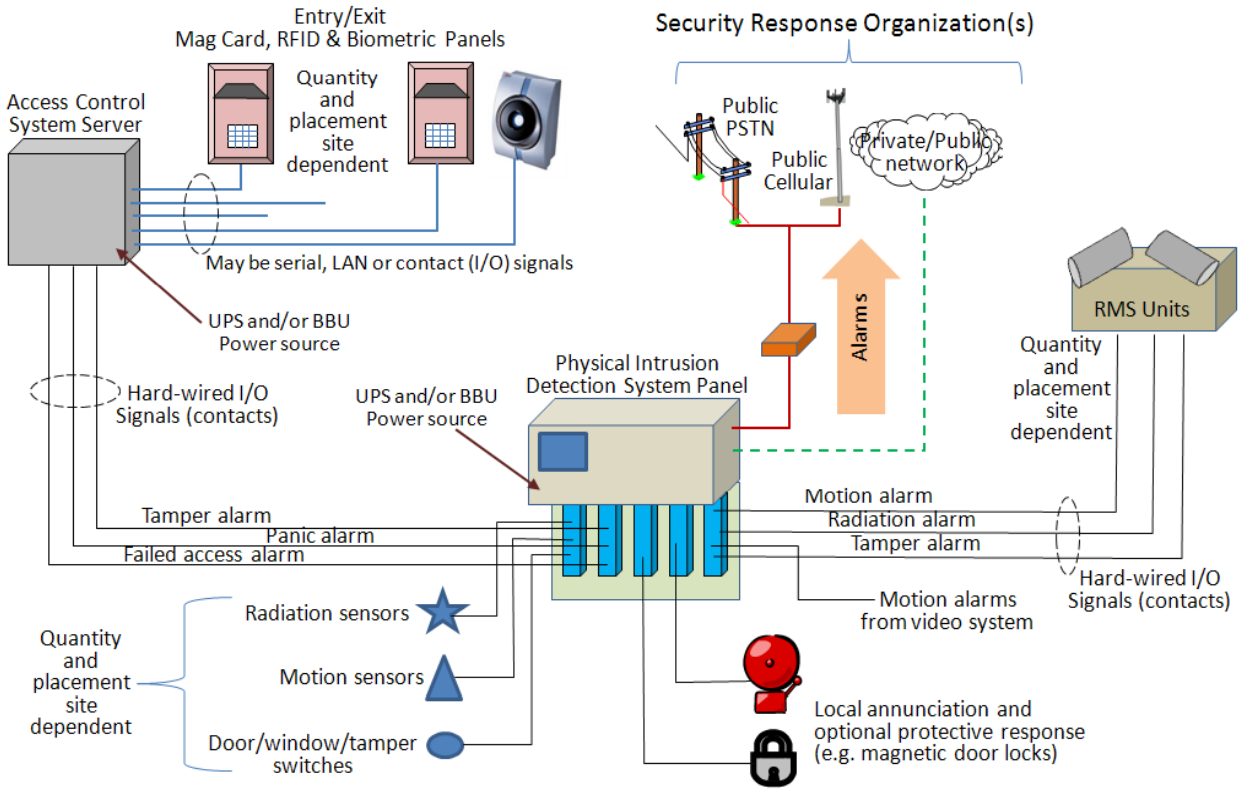
Cyber security requires adequate physical security

- Physical security is enhanced by digital systems
- Those systems need adequate cyber security



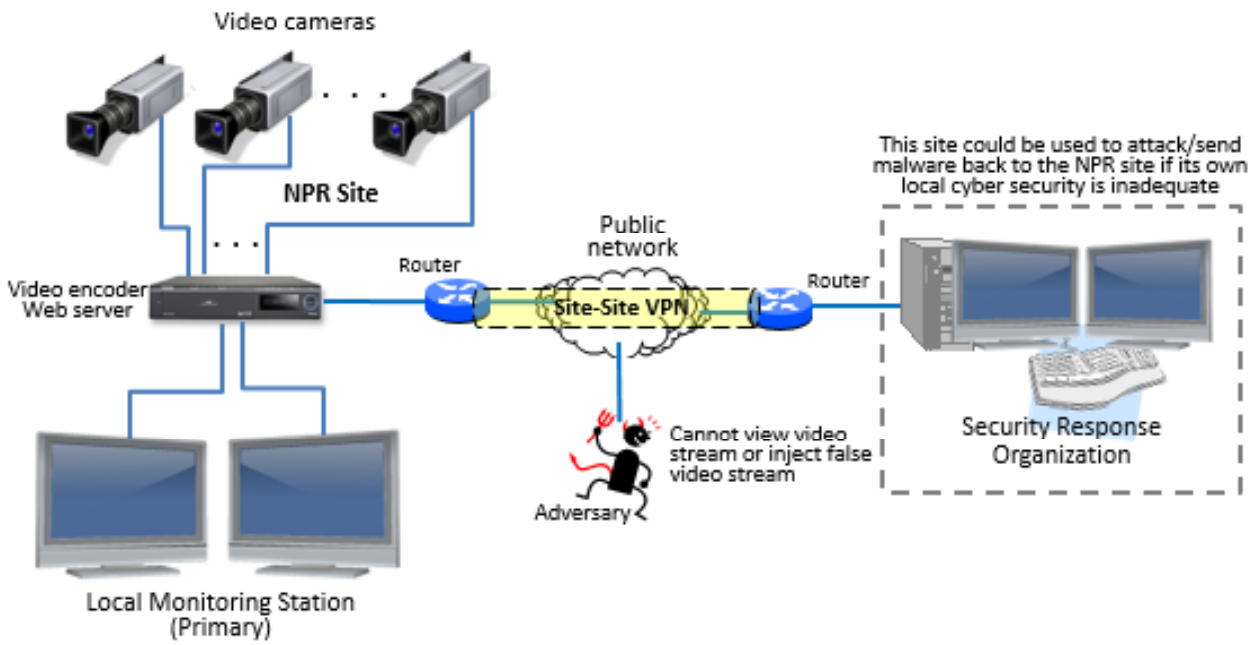
Security Systems

Access control and Physical intrusion detection and alarm systems offer a potential cyber target. Several effective practices are offered in regards to their protection



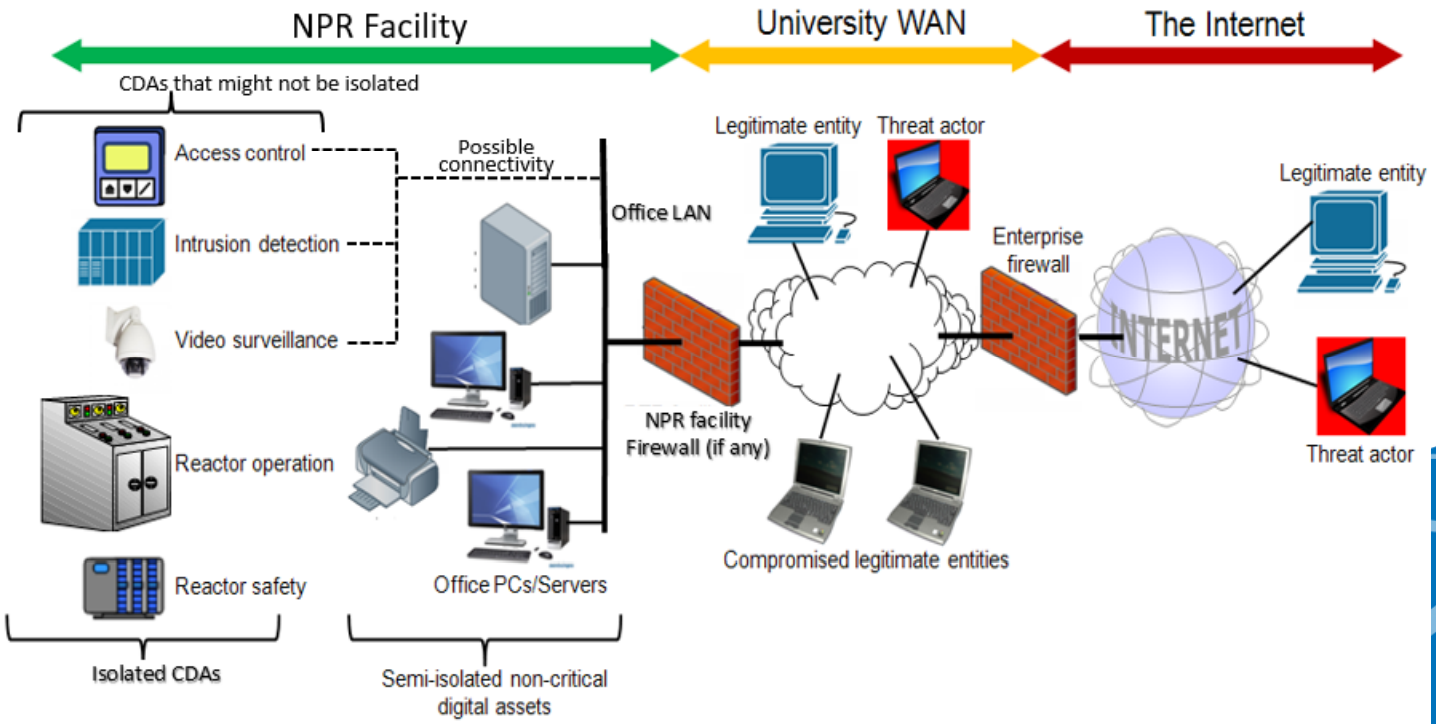
Security Systems (cont'd)

Video surveillance systems are also important for physical security and for incident response personnel. There are ways to protect such systems against cyberattack



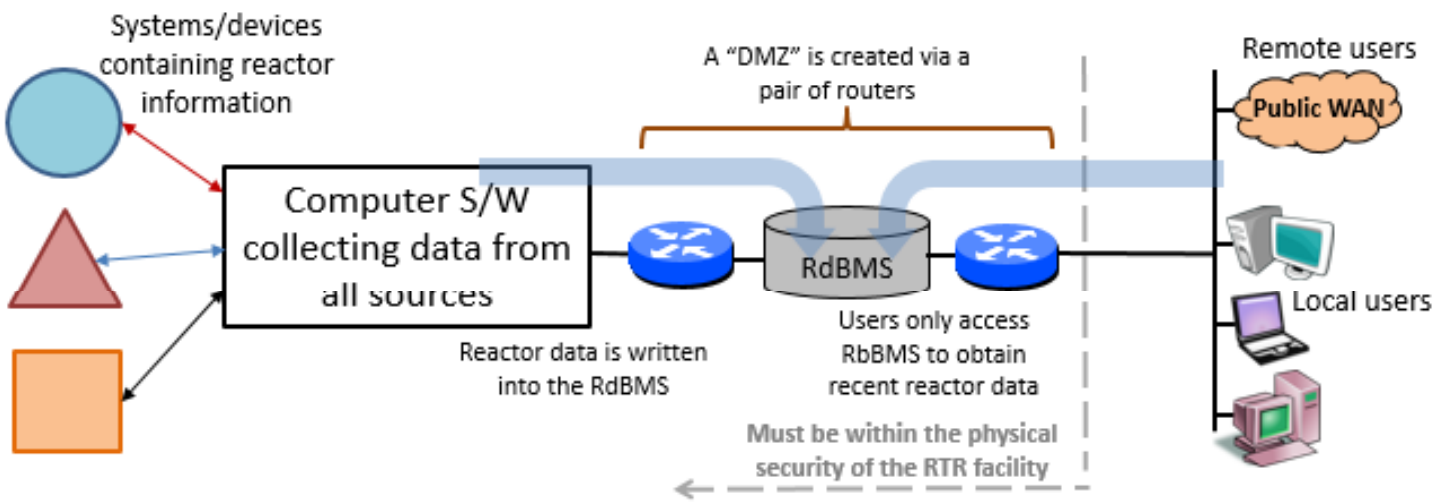
Facility Architecture

The survey of NPR facilities revealed many similarities and some critical differences in the way in which NPR facilities are connected to, and protected from, the outside world. Some ways are more cyber effective than others.



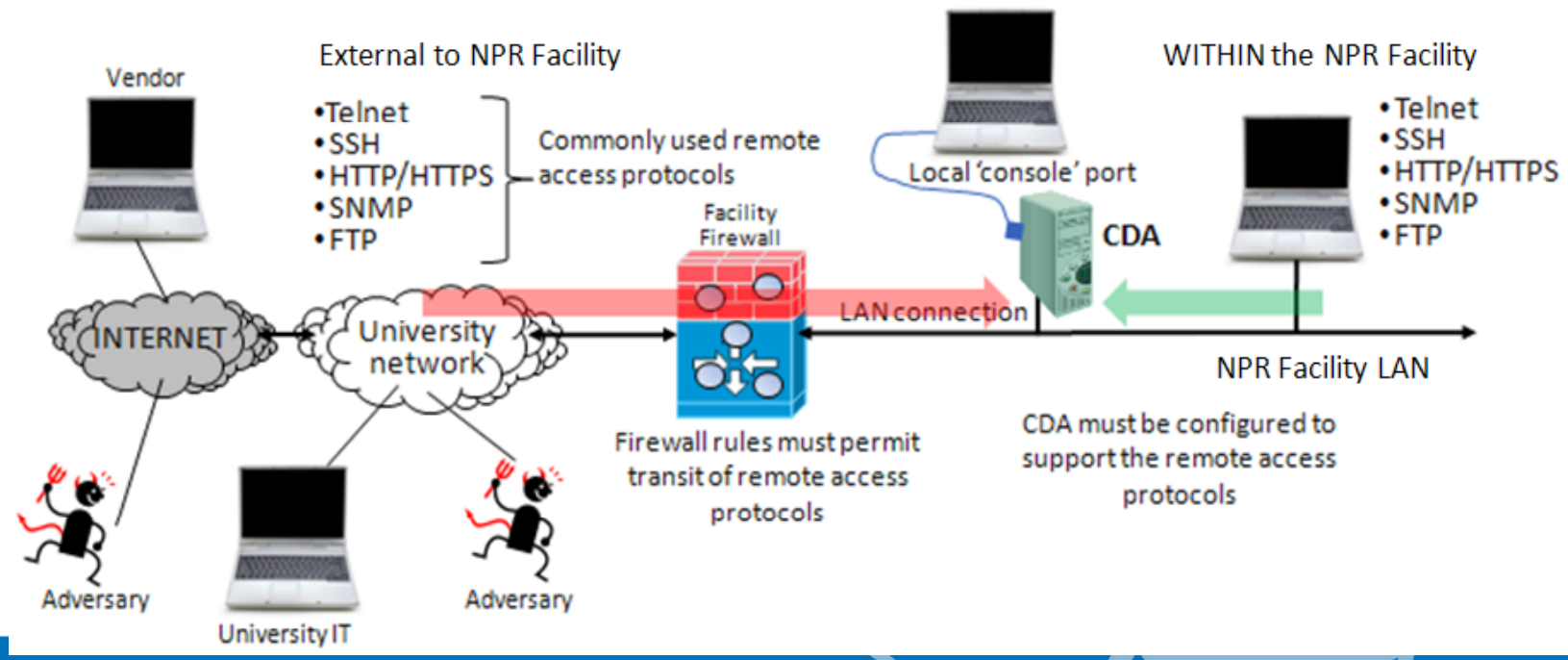
Interconnectivity

Most of the surveyed licensees want to provide information flow, in real time, to external remote users. There are ways to do this in a cyber secure manner. Possible approaches for achieving this in a cyber secure manner are described in the document

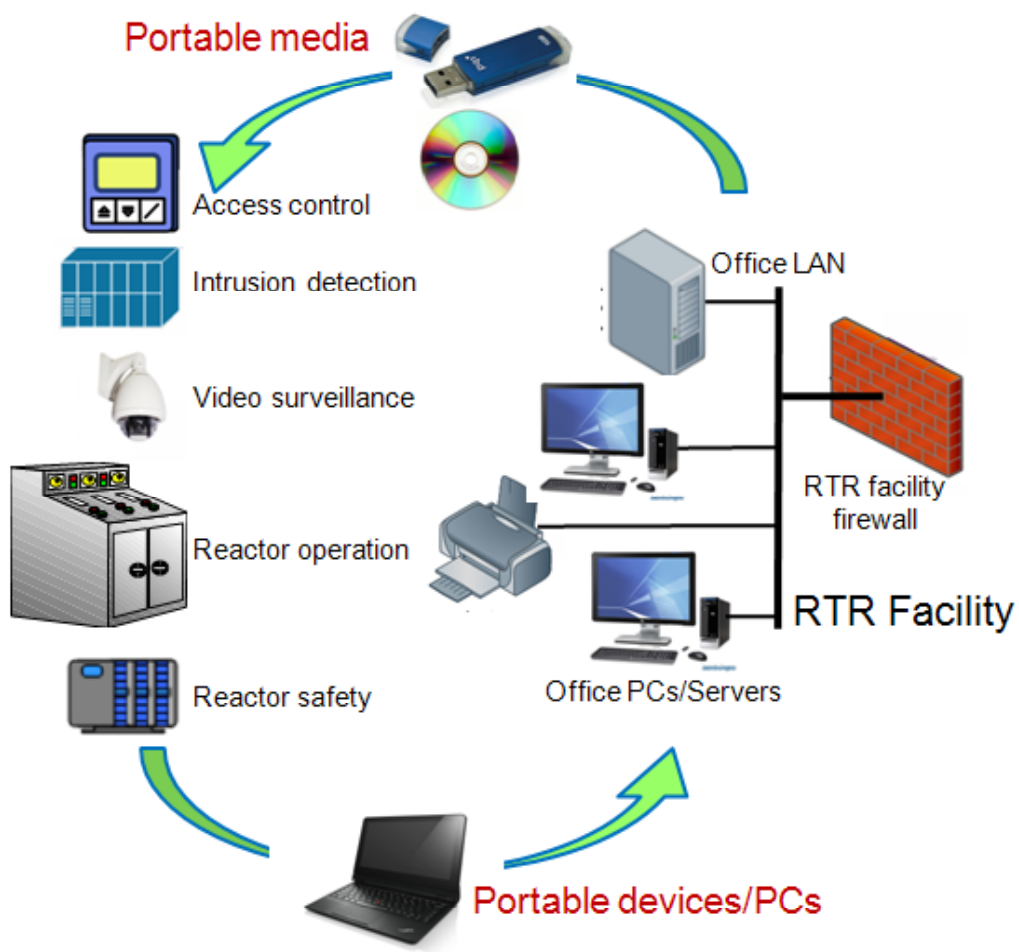


Administration

Many NPR sites depend on University IT and vendors to provide remote technical support and system administration. There are cyber secure and cyber insecure ways to implement this capability.



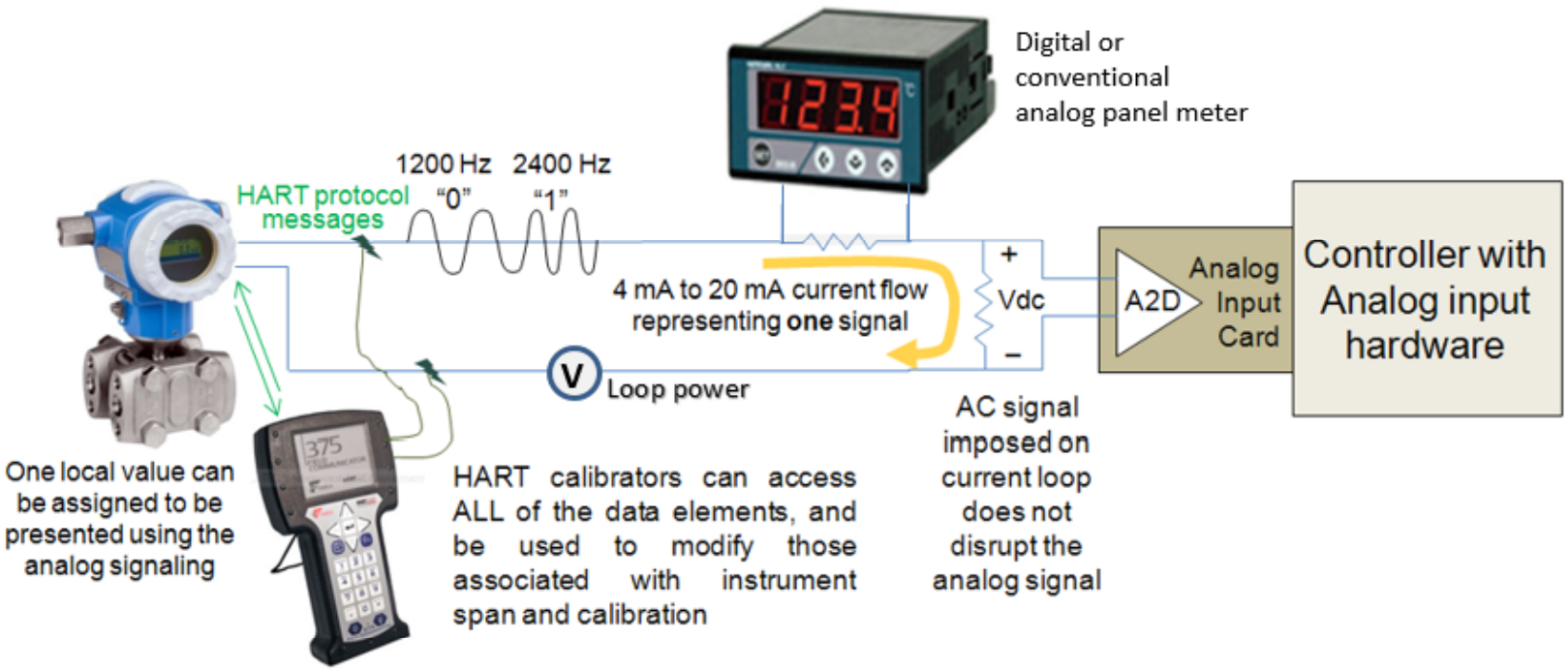
Portable Media



Portable computer readable media and portable computer devices continue to be a major attack vector for delivery of malware but there are effective practices that can reduce the threat posed by these devices

Digital I&C

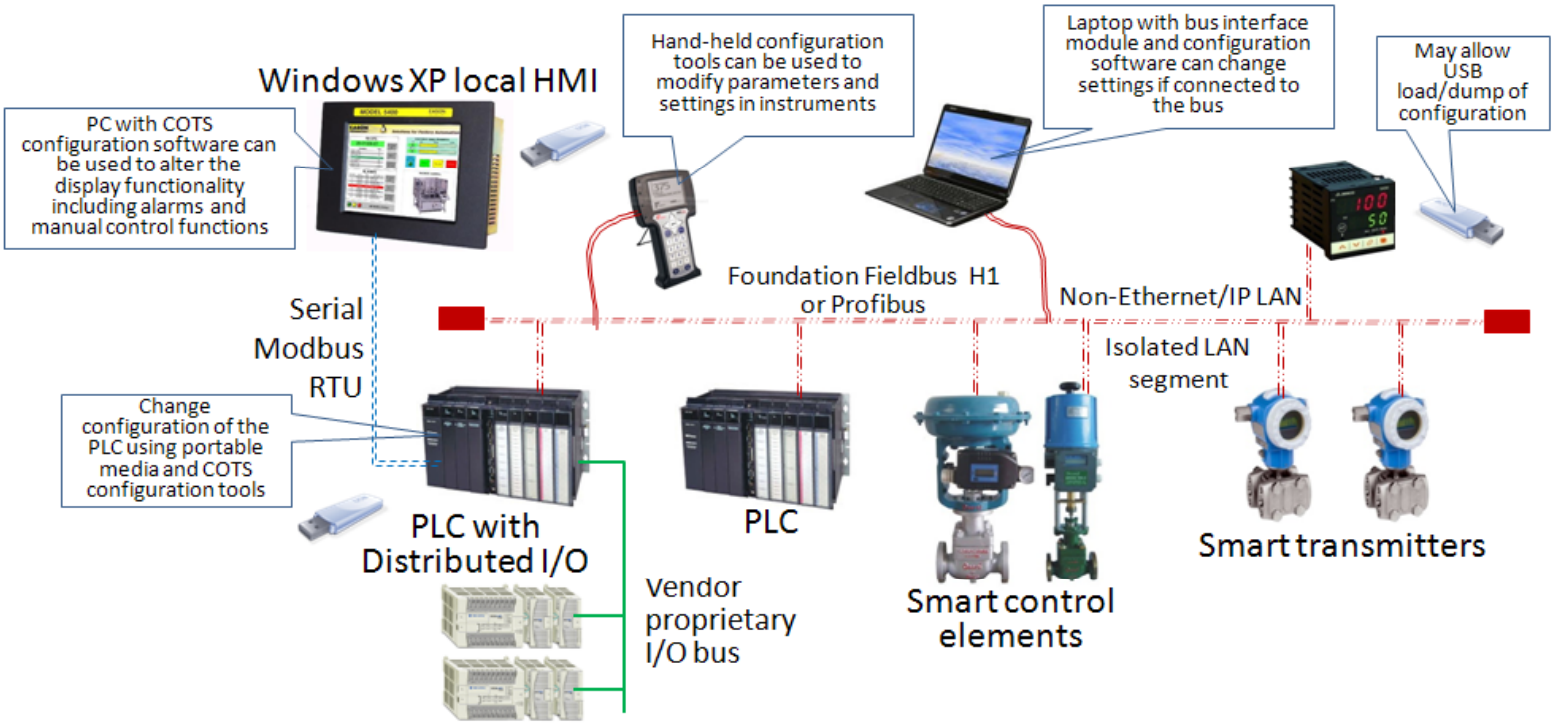
Digital instrumentation and control systems can be applied in a manner that retains the required safety and security of the NPR. This topic is extensively discussed in chapters 10 & 11



Digital I&C (cont'd)

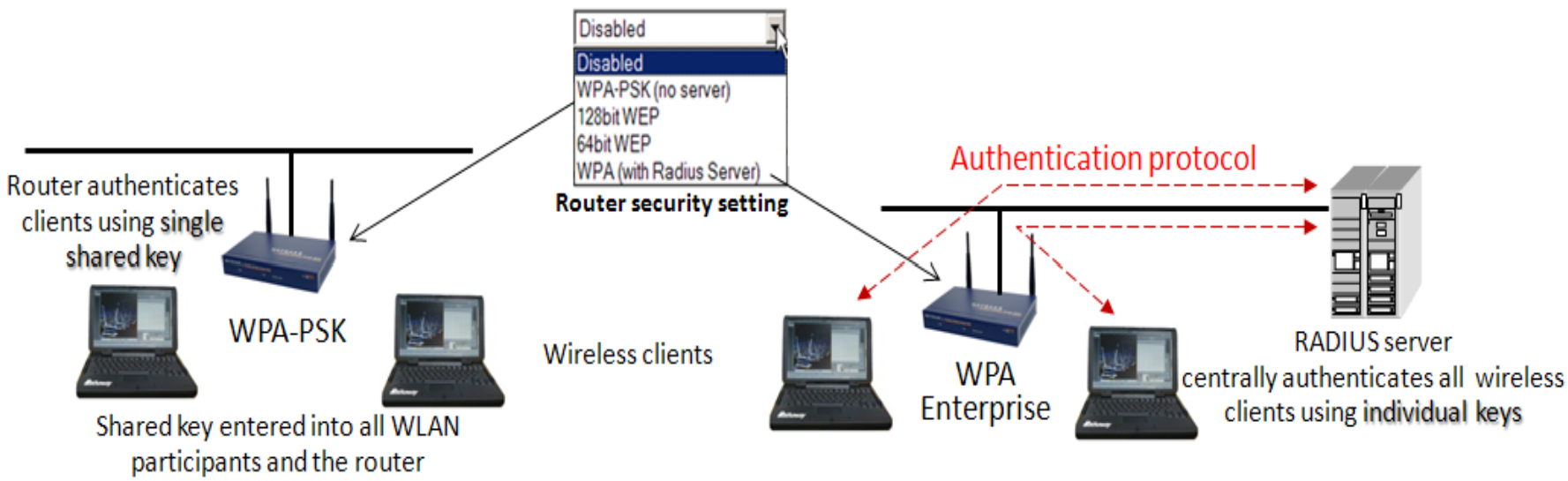
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital instrumentation and control systems create opportunities for cyber tampering and manipulation but there are effective practices that greatly reduce the potential cyber vulnerabilities

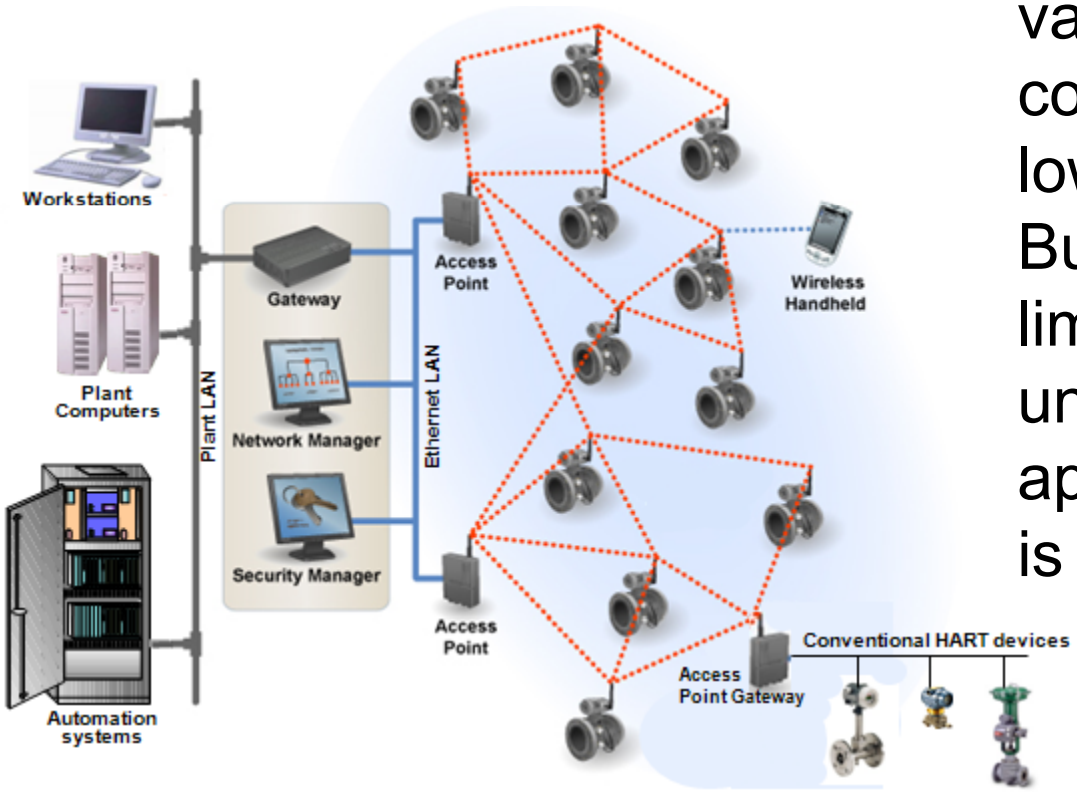


Wireless LANs

Some NPRs use wireless Ethernet (WiFi) within their facility and wireless LANs can be implemented on a manner that provides strong cyber security. But this requires an understanding of the security trade-offs. There are effective practices for use of WLANs in a cyber secure manner



Wireless Instrumentation



Digital instrumentation today includes wireless variations that offer convenience, flexibility and lower cost of installation. But they also suffer from limitations that need to be understood. Effective application of such devices is discussed

Digital Replacements

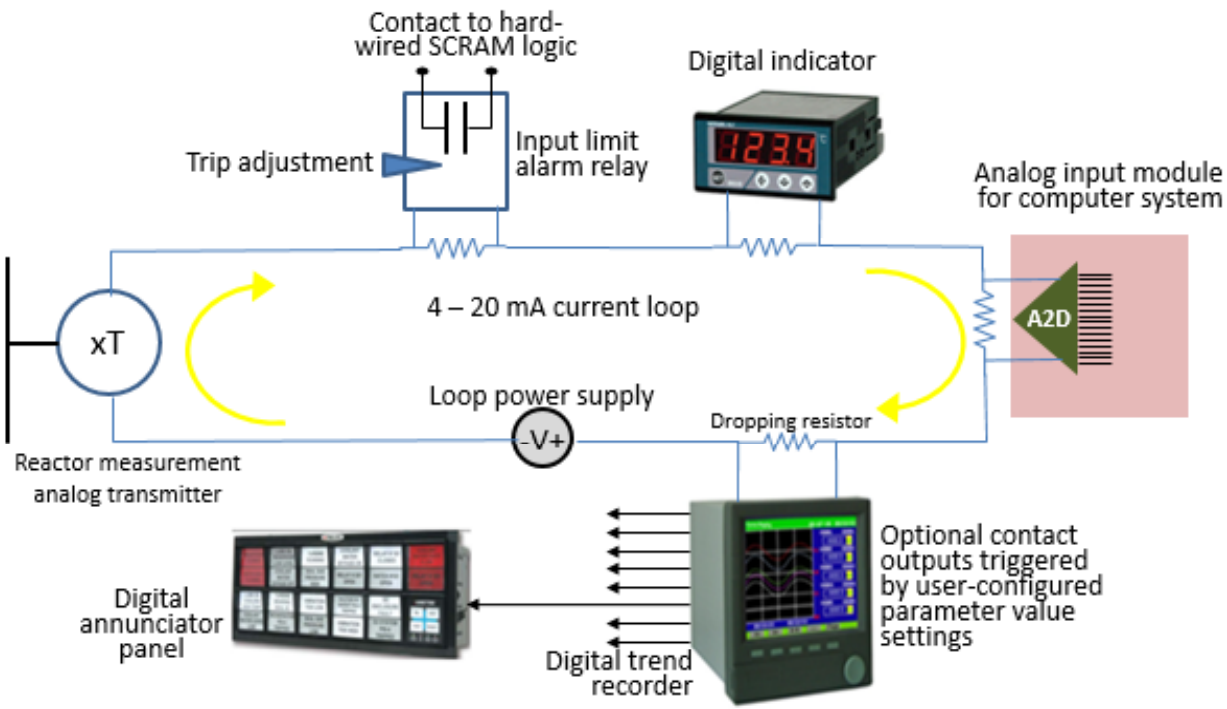
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Many licensees have begun replacing control panel devices with digital replacements. These come with capabilities that can be cyber exploited. But there are effective practices that make it possible to perform such replacements without creating a cyber security vulnerability

Analog instrument		Digital Equivalent	
Chart recorder	Attributes	Trend recorder	Attributes
	Eight 4-20 mA inputs Adjustable scale and zero offset ('trim pots')		Eight 4-20 mA inputs Ethernet MODBUS/TCP Eight contact outputs Programmable trip-points Configurable plot scaling USB Bulk memory storage Menu-based configuration
PID controller	Attributes	PID controller	Attributes
	4-20 mA input 4-20 mA output PID only Local (manual dial) setpoint Local ('trim-pots') loop tuning		4-20 mA input 4-20 mA output HART communications Configurable for P,PI,PID, error-squared or R+B Remote setpoint via HART Remote loop tuning via HART

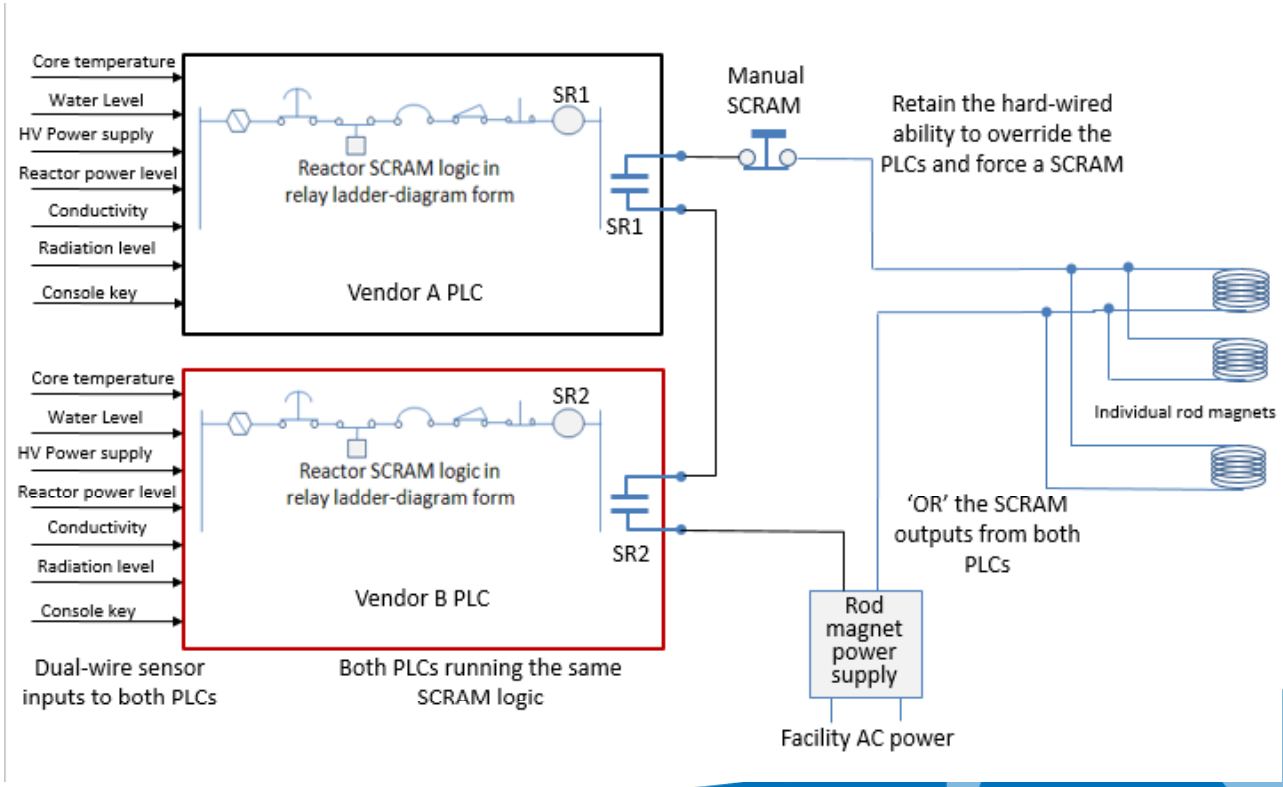
Upgrade/Replacements

There are possible ways to integrate digital technology into both reactor operations and reactor safety without reducing the existing level of reliability and availability. Effective practices for doing so are discussed with some of the possible ways in which this can be achieved



Upgrade/Replacements (cont'd)

Many licensees have asked about replacing the hard-wired (mercury-wetted relay based) reactor safety systems with a modern digital device. Effective practices and possible approaches that might provide adequate reliability and cyber security are discussed in the document



Basic Criteria

- *In general terms the most important consideration and effective practice, from a cyber security perspective, when applying ANY digital/computer technology is to ensure that a malfunction (accidental or malicious) of that technology (all or part) cannot prevent/block the reactor safety system (or operator) from performing a SCRAM.*
- *The second most important consideration is to ensure that reactor operators have a diverse means of seeing the current values of essential reactor operating parameters so that a malfunction (accidental or malicious) in any digital device/subsystem cannot 'blind' the reactor operator to the true value of any of those reactor operating/safety parameters.*

Current Reality

The NRC recognizes that NPR facilities currently face a transition point - most are attempting to maintain their operations using non-digital and increasingly obsolete computer technologies with the spare parts needed to support them either no longer available or becoming scarce. In order to maintain their operations into the future, most NPR licensees will need to adopt commercially available digital instrumentation and control (DI&C) and computer-based automation technologies.

Current Reality (cont'd)

Beyond merely maintaining their operations, many licensees have indicated that they could enhance their research activities and improve operational efficiency by the judicious application of available digital technologies.

Future Trends

Looking at just the reactor systems possible digital enhancements could include:

- "Smart" instrumentation and instrumentation LANs
- Digital signal processing technologies
- Relational database information storage
- PLC and PAC microprocessor controllers
- User-configurable operational displays
- Commercial SCADA/HMI software
- Web-based informational/operational displays
- Smart alarming/alarm management
- Equipment condition monitoring
- Biometric authentication (operator)
- Automated reactor diagnostics
- Autonomous regulatory control
- Mathematical models and model-based control

83 Effective Practices

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

EP#43 – Where remote (cross-network) access is allowed for administrative and/or maintenance support of CDAs, because of the need to allow for firewall rules to pass such traffic, an effective cyber security practice would be to install a network intrusion detection system (NIDS) on the NPR facility LAN in order to inspect all message traffic entering and exiting in order to identify malicious, suspicious, unauthorized and questionable messages and provide a notification to appropriate NPR administrative personnel.

The document specifically includes 83 effective practices ranging from simple procedural changes all the way up to possible IT cyber security practices that would be most effective.

EP#60 – An effective cyber security practice is to never connect portable digital devices to CDAs via USB without first running an AV scan on their file system (possibly by connecting them to a separate computer designated and configured for this purpose.)

Summary

The overall purpose of this effective practices document is to provide NPR licensees with information about how to utilize digital I&C technologies and modern computer and networking technologies in a manner that provides adequate cyber security protections and mitigates the risks

Summary (cont'd)

These effective practices are directly applicable to:

- Reactor safety
- Reactor operational systems
- Physical security support systems

Questions?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment